UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/880,231	06/12/2001	Ron Karim	15437-0508	5058

45657 7590 10/04/2006

HICKMAN PALERMO TRUONG & BECKER, LLP
AND SUN MICROSYSTEMS, INC.
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110-1089

EXAMINER	
WU, QING YUAN	

ART UNIT	PAPER NUMBER
2194	

DATE MAILED: 10/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/880,231	KARIM, RON	
	Examiner	Art Unit	
	Qing-Yuan Wu	2194	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-17 and 20-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-17 and 20-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 4-17 and 20-32 are pending in this application.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 4-17 and 20-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schnurer et al (hereafter Schnurer) (U.S. Patent 5,842,002), in view of Nachenberg (U.S. Patent 6,357,008), and further in view of Basu et al (hereafter Basu) (U.S. Patent 6,836,888).

5. Schnurer and Nachenberg were cited in the last office action.

6. As to claim 1, Schnurer teaches the invention substantially as claimed including a computer-implemented method for executing an untrusted program [abstract, lines 1-2], comprising:

establishing a limited environment within a general environment [col. 6, lines 56-58; Figs. 3 and 4], wherein said limited environment comprises one or more mock resources [col. 4, lines 16-20, 22-26 and 47-49; col. 7, lines 3-8], wherein said general environment comprises one or more real resources [col. 4, lines 24-25; col. 7, lines 15-18], wherein programs executing within said limited environment cannot access the one or more real resources in said general environment [abstract; col. 5, lines 5-10; col. 7, lines 15-18];

executing at least a portion of an untrusted program within said limited environment [col. 7, lines 5-12]; and examining said limited environment after execution of at least said portion of said untrusted program to check for undesirable behavior exhibited by said untrusted program [col. 4, lines 32-36; col. 7, lines 12-15; 48, 50, 52, Fig. 1].

7. Schnurer does not specifically teach wherein said limited environment and said general environment are both provided by the same operating system. However, Schnurer disclosed trapping device within a network environment [col. 6, lines 56-58; Fig. 3 and 4]. In addition, Nachenberg teaches an antivirus program that includes a decryption, exploration and evaluation phases/modules causing a CPU emulator with virtual memory to simulate untrusted programs/instructions [Nachenberg, col. 1, lines 16-20; col. 5, lines 27-40; col.6, lines 52-58; col. 7, line 31-col. 8, line 47].

8. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have combined the teaching of Schnurer with the teaching of Nachenberg by implementing the limited environment in the same machine as the general environment if the limited environment is limited to protect a specific machine and to have an operating system within the machine providing both environments for the same reason to avoid the overhead of communicating through a network (i.e. an antivirus program running under an operating system protecting other programs/hardware/real resources running under the same operating system).

9. Furthermore, Schnurer and Nachenberg do not specifically teach wherein said limited environment is a shell in a UNIX operating system environment. However, Nachenberg disclosed different operating systems [Nachenberg, col. 6, lines 52-58]. In addition, Basu teaches a shell program as a user interface to a sandbox in a UNIX operating system environment [Basu, col. 9, lines 17-22; col. 12, line 66-col. 13, line 5].

10. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have combined the teaching of Schnurer and Nachenberg with the teaching of Basu because the teaching of Basu can further increase the flexibility of Schnurer and Nachenberg's system by implementing the limited environment on different operating systems.

11. As to claim 4, Schnurer as modified teaches the invention substantially as claimed including wherein examining said limited environment comprises: determining whether a mock resource has been deleted [col. 4, lines 37-39; col. 7, lines 12-15; Nachenberg, col. 9, line 44]. Schnurer as modified does not specifically teach a particular mock resource. However, Schnurer disclosed if anything within the environment changes, is a sign of a virus [col. 7, lines 48-52], and Nachenberg disclosed signature scanning of known viruses [Nachenberg, col. 1, lines 22-45]. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that a deletion of a particular file such as a system file is an obvious sign of a virus (i.e. deletion of a particular system file that would cause instability to the operating system).

12. As to claims 5-7, these claims are rejected for the same reason as claim 4 above. In addition, Schnurer as modified teaches mock resource has been renamed or moved [Nachenberg, col. 9, lines 47-49], or altered [col. 7, line 48 to col. 8, line 26; Nachenberg, col. 9, lines 54-55].

13. As to claim 8, Schnurer as modified teaches the invention substantially as claimed including wherein said mock resource has a parameter associated therewith which changes when said mock resource is altered, and wherein determining whether said mock resource has been altered, comprises:

determining whether said parameter has changed [col. 7, line 48 to col. 8, line 26].

14. As to claim 9, Schnurer as modified does not specifically teach the step of determining whether said mock resource has been last updated. However, Schnurer disclosed that his system could detect any malicious act by the virus, including the activities of changing the FAT table and changing of the error checking algorithm [col. 7, lines 59-60; col. 8, lines 25-26; col. 4, lines 37-39]. It would have been obvious to one of an ordinary skill in the art at the time the invention was made, to have recognized that common viral activities or critical behaviors exhibited by viruses would have included the updating of system resources as being considered and implemented in Schnurer et al's method of virus detection.

15. As to claim 10, this claim is rejected for the same reason as claim 4 above. In addition, Schnurer as modified teaches the invention substantially as claimed including wherein examining said mock environment comprises:

determining whether said mock resource has been accessed [col. 7, line 48 to col. 8, line 26].

16. As to claim 11, Schnurer as modified does not specifically teach wherein said mock resource contains one or more sets of content, and searching a particular portion of memory for at least one of said one or more sets of content. It is well known in the art that when a file gets accessed or altered, traces of the contents being accessed is located in the memory, in addition, Schnurer disclosed the determination of potential viral activities by examining "if anything within the environment changes..." [col. 7, line 48 to col. 8, line 26].

17. As to claim 12, Schnurer as modified teaches the invention substantially as claimed including providing information indicating behavior exhibited by said untrusted program [col. 7, line 25 to col. 8, line 26].

18. As to claims 13 and 14, Schnurer as modified teaches the invention substantially as claimed including wherein said information comprises indications of undesirable behavior exhibited by said untrusted program [col. 7, lines 48-52], and in response to a determination that said untrusted program has exhibited undesirable behavior, taking corrective action [col. 8, lines 27-35; 52, Fig. 1].

19. As to claims 15 and 16, Schnurer as modified teaches the invention substantially as claimed including wherein taking corrective action comprises: deleting said untrusted program and warning to a user [col. 8, lines 27-35; 52, Fig. 1].

20. As to claims 17 and 20-32, these are system claims that correspond to the method claims 1 and 4-16. Therefore, they are rejected for the same reason as claims 1 and 4-16 above.

21. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 6,907,533 to Sorkin et al teach honey pot/virtual cage environment within a general environment.

Response to Arguments

22. Applicant's arguments filed 7/7/06 have been fully considered but they are not persuasive.

23. In the remarks, Applicant argued in substance that:

a. Schnurer would be destroyed if the Examiner's proposed suggestion were to be carried out.

b. The feature of "wherein programs executing within said limited environment cannot access the one or more real resources in said general environment" could not be shown by Schnurer.

24. Examiner respectfully traversed Applicant's remarks:

25. As to point (a), this argument was addressed by the advisory action dated 6/7/06. Therefore, applicant's argument is not persuasive.

26. As to point (b), Applicant failed to explain why the mapping of the examiner's rejection based on Schnurer do not meet the claim limitation. Schnurer clearly teaches wherein programs executing within said limited environment [virus performing its intended activity within virtual world, abstract] cannot access the one or more real resources in said general environment [access to the real world is completely blocked, abstract; col. 5, lines 5-10; col. 7, lines 15-18].

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Qing-Yuan Wu whose telephone number is (571) 272-3776. The examiner can normally be reached on 8:30am-6:00pm Monday-Thursday and alternate Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Thomson can be reached on (571) 272-3718. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Qing-Yuan Wu

Examiner

Art Unit 2194

WILLIAM THOMSON
SUPERVISORY PATENT EXAMINER